Response1: It's difficult to respond without a definition but, while "digital identity checking" is ***a*** way, (and why attribute-checking has become popular), it's poor practice to:

- over-identify: use more information than minimally necessary to mitigate the identity-related risk,
- use identification when unnecessary (e.g. in many entitlement use cases), and
- identity check individuals and organisations multiple times – instead RPs should use either federated trust frameworks or trusted/verified self sovereign decentralised identifiers (a previously checked entity with an electronic credential bound to its identification doesn't need to be rechecked).

Response2: A digital identity/identification "system" isn't an end in itself. It's a means to lower friction and increase economic velocity in the digital economy through safe, secure, private and, to the extent possible, user-directed practices. It's not a single system, it's multiple interoperable systems with common plumbing – code libraries, function sets, web apps – for developers to mix and match/plug and play to tailor customer solutions. Not developing something approximating "a digital identity system" incurs the cost of:

- fraud,
- rebuilding an online identity,
- loss of trust and confidence,
- slower economic velocity, and
- impeding the adoption of the digital economy.

Response3: Typically, the process of identification – self claimed, second or third party checked – involves verification of presented information. While "identity verification" isn't defined, the two aren't synonymous as implied.

Industry believes that Verify pays IdPs £20/verified person while IdPs' direct costs are around £5/verified person. The difference is partly explained by the significant indirect cost of integrating with Verify and a "risk factor" built into the price to offset their lack of control of future government policy shift. The current model incents IdPs to duplicate user enrollments which increases taxpayer cost and user management burden. The cost and burden of approaching the challenge like is made worse by the fact that identity verification alone doesn't usually give an RP sufficient confidence to grant access to a resource, requiring them to process additional attributes with requisite incremental cost. Graduated adoption of SSI as it matures would disintermediate IdPs and detract the government from its fixed architectural mindset.

Response4: Inclusion cannot be ensured but it can be improved using multiple standardised compensating controls to meet GPG requirements. For the thin file segment, building confidence over time (e.g., collecting additional attributes from non-authoritative sources can reduce identity related risks for a transaction) enables assurance levels to graduate upwards so higher risk transactions can be tested. Not everything can be made digital to suit every audience at any given time of market and technology maturity. One size does not fit all, in this space.

Response5: The notion of a "digital identity market" doesn't give IdPs or RPs sufficient flexibility, incentive, return on investment or risk mitigation confidence to address their respective customer segments – at least in the existing hub model. Each IdP builds its own system from open source code libraries and/or proprietary software. Government can help by facilitating code libraries for protocols,

messaging, APIs etc – all pre-checked for interoperability, bugs etc – that are off the shelf, free and unencumbered by proprietary licences so developers don't have to develop and integrate bespoke code as is the case with Verify today. Complexity and investment come at the technical, policy, sector and business process orchestration layer. Orchestration is the enabler across different domains (finance - health - government) which leads to convergence, if not, interoperability and increased confidence to invest.

Response6: Life events, where a combination of government and non-government-based services combine into a typical user journey, is an obvious start. While there are hundreds of these beyond the usual birth-death-marriage, digital identity may only play a small part. From benefit entitlement on one hand to skills/qualification-based admission entitlement on the other, personas and relevant attributes are more necessary than full identification.

Response7: From the consumer perspective, trust is seen as:

- how often they use a branded service without harm or undue friction,
- how well their privacy, security and data are protected and,
- for some, how much agency they have over their data.

An individual consumer seeking a friction-free digital transaction experience, doesn't normally care about universal coverage (free to the public), standardisation, social inclusion, legality, nor proven liability models unless they directly affect them. This is the domain of policy specialists. Nonetheless, consumers expect government to enable policies that act in their individual best interests.

While open standards play an essential role, they, alone, don't create or build trust. While consumers might not care, government should care because they enable a digital economy that can be trusted in the minds of the consumer. Standards need to be community developed, freely available, deployed, and interoperable that are implemented by service providers that are trust marked with evidenced conformance and assurance against the standard. Government should set the high-level conditions, support their enforcement and buy industry-wide licences for chargeable standards from BSI if they won't support the few industry associations like Kantara, that offer low or no barriers to participation and adoption of specifications.

Response8: When implemented with consistent quality they help build consumer trust by enabling less problematic user online experiences, while also building ecosystem trust amongst the participants due to the equality that these activities engender. Assurance and certification of a service is useless without assurance of an organization's underlying ISMS policies, procedures and risk posture. Self asserted assurance is too easily gamed in identification and credentialing processes though less so in technical protocol conformance.

Response9: Enabling a principles and outcomes-based policy/legislative framework that has real meaningful enforceable consequences – fines and "public shaming" – will ensure that activities, such as the use of innovative technologies (e.g. biometrics), operate in a manner that protects the privacy of users. Privacy Impact Assessments, together with assessment criteria to ensure consistency of results, is core to addressing this challenge.

Response10: Assessment and certification, together with enforceable consequences for non-compliance, is essential. Graduated introduction of suitable identification and authentication techniques applied as compensating controls against the standards can assist people with protected characteristics.

Response11: Meaningful and enforceable consequences for non-compliance is essential. An ombudsman should be appointed to facilitate disputes. An operations focussed group comprising private, non-profit and public sector representatives from the respective roles of the ecosystem as well as government representatives from applicable policy and regulation agencies (ICO etc) should work in an open transparent partnership covering:

- policy, governance, codes of practice,
- standards and specifications, and conformity assessment and assurance of those,
- code libraries, protocol "plumbing", messaging, interoperability test suites, APIs etc.

Response12: Putting aside the assumption of "a market", with which Kantara disagrees, the UK Government should redouble private/public sector stakeholder collaboration (per Response11) informed by comparable efforts internationally. Success is dependent upon the ability to manage divergent motivations while defining clear lines of responsibility when setting the rules framework. While an improvement over past efforts, the Canadian DIACC initiative isn't yet an outstanding success as the public and private sectors seem to be "taking their own paths" with the implementation of the Pan-Canadian Trust Framework. Such underlying dynamics need to be understood. Finland offers the most recent attempt at a business model. "Rules of the road" should use current legislation as their baseline (no reinvention or duplication please) and address legislative gaps/required extensions to build a more integrated and harmonious digital identity ecosystem responsive to, and reflecting, current regulation. This ecosystem is not the special snowflake some advocate that it is.

Response13: the following should be involved:

- operationally engaged stakeholders, plus those with demonstrable previous operational experience from the UK or abroad,
- agencies that represent the legislation/regulation applicable to digital identity, and
- most importantly, consumers of the services - through civil society representatives and directly via focus groups (to learn from their user experience).

Response14: Yes, but see Response1 and Response20. Use of government documents and/or their associated attributes has to be carefully/cautiously considered as to whether information collected to issue the government document can be used for the purpose of identification. For example, validation of specific attributes for passport issuance, most jurisdictions' legislation cites that information collected is for the sole purpose of validating that the applicant can be issued a passport. Without prior consent, the use of these attributes for different purposes likely violates privacy protection principles/legislation. Indeed attributes may not be needed. A simple yes/no answer from an authoritative source to the presented attributes helps assure identification and protects privacy.

Response15i: Validity checking of government-issued documents (or their attributes) should only be opened up where the attributes are needed to address a transaction's or entitlement's identification-related risk to access government services, cross border activities, or fulfilling regulatory requirements (e.g., KYC/AML for opening a bank account). Purposes must be proportional to the risk to be mitigated (data minimalisation and protection principles).

Response15ii: There is abundant existing legislation and enforcement – for citizens and non-citizens - that can be supported with directed use of PETs backed by assurance, audit and certification. Ecosystem industry sectors should address non conformance through:

- self regulatory codes of conduct,
- whistle-blowing.
- an open, transparent, operationally efficient public complaints system.

Response15iii: Most models have been costly for one or more parties or have failed. The newest model (Finland's) shows promise. Pilot a range of options including a low value transaction-based option, provided they are transparent to the entire ecosystem and capable of scale. Don't impose anything; let ecosystem participants determine what's best for them.

Response16i: See Response14 and Response15i. It's for services, transactions and entitlement where a RP's identity-related risks could be mitigated by these attributes (e.g. age) and most services only require an 'over/under' assertion – not age or even date of birth.

Response16ii: Response15ii applies, with some differences depending on context and whether the source used is authoritative or derived.

Response16iii: See Response15iii.

Response17: Legislation and regulation must include meaningful and enforceable consequences to ensure that players act appropriately while giving room for innovation with progressive introduction. There is already common, commercial and privacy/data protection law for electronic commerce. Digital identification doesn't need its own laws. Use self regulation and third-party audit to support existing legislation.

Response18: Kantara makes three general recommendations:

1) Undertake a legislative review to determine existing identity-related requirements, then modify legislation repurposing for digital identification.
2) Analyse machinery of government, shared services funding policy and inter-agency rivalry for impediments to digital identification and remediate.
3) Support electronic signatures bound to good identity proofing, to enable more digital identification.

Response19: Kantara recommends that Government:

- be an early adopter,
- incentivise organizations offering services incorporating digital identification,
- support the profiling of existing standards and assurance,
- allow central and local government agencies to plot their own course for their consumer segments within enabling policy and not take control away,
- incentivise individual agency over data, understanding that identification data is personal data,
- champion transparency of costs and liabilities, cross border interoperability and cross sector sharing.

While government leads in funding digitally delivered services, the direction and agenda should be set by the private sector, even if it is primed, in part, by government.

Government needs to ensure that it doesn't, even unintentionally, create Conflicts of Interest. While there may not be maleficence, perception and optics can disincentivise others to engage. Kantara believes perceived Conflicts of Interest form if government takes a seat as a Board Director and/or appears to be exclusively providing funds to just one or two industry consortia and/or doesn't meaningfully engage with others.

Response20: Digital identification can, and should, support local government – e.g. library cards and concessionary travel. However, identification should only be applied where the identity related risk warrants it. Only attributes giving confidence that a requestor is entitled to the service need be asserted. Consider deploying Kantara's User Managed Access specification implemented internationally.

Response21: While partly overlapping the public sector's needs, the private sector has different dynamics. It needs to engage in creating trust models. Non-pay-to-play industry associations should be used as neutral facilitation vehicles to maintain the cohesion and sustainability of trust models. Industry associations vary significantly in ethics, ethos, mission and scope, so entities should be able to choose with which they align. Government should ensure all industry organisations are equitably represented.